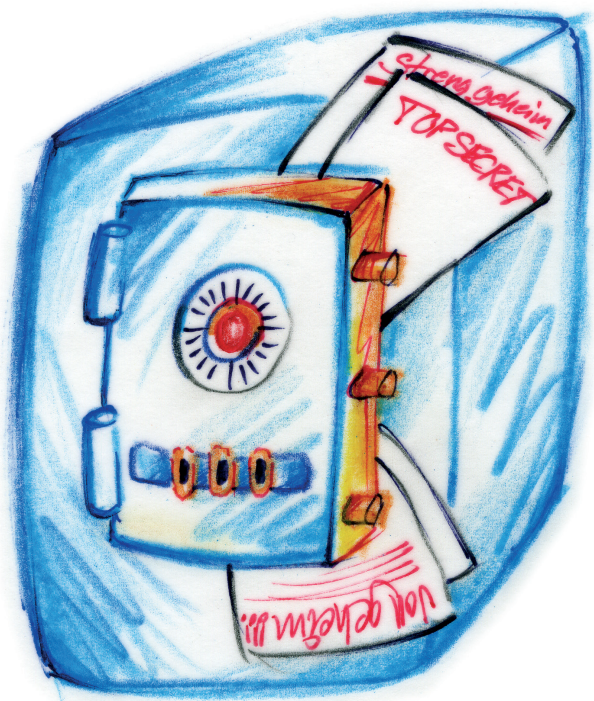


Data Protection Instructions

Information for Employees of KIT

DATA PROTECTION CONCERNS US ALL!



Dear Colleagues,

Progressing digitization of personal data, increasingly complex IT infrastructures, and increasing cross-linking of stored data have made data protection an indispensable and integral part of our acting and a high priority in our society.

Correct use of personal data also is an important and central concern of Karlsruhe Institute of Technology (KIT).

With the adoption of the EU General Data Protection Regulation (GDPR), data protection legislation was standardized throughout the European Union. The GDPR is directly applicable and does not have to be implemented in national law. National legislators were authorized, however, to define in more detail and supplement certain provisions of the GDPR by own data security regulations. The German legislator exercised this option. Hence, not only the GDPR, but also the State Data Protection Act (LD SG) for Baden-Württemberg have been applicable to KIT since June 21, 2018.

The present brochure is to facilitate correct handling of personal data at your new workplace. You will find information on basic concepts and principles of data protection and persons to contact in case of questions. In addition, information is provided as to how you can contribute actively to data security by taking some simple measures.

Your Data Protection Commissioner of KIT

General Information

DATA PROTECTION PURPOSE

Every person in principle has the right to decide on the disclosure and use of his/her personal data.

This right to informational self-determination (Federal Constitutional Court, judgement of December 15, 1983, BVerfGE 65,1) represents a special expression of the general right to the protection of personality as outlined in Article 2, par. 1, in conjunction with Article 1, par. 1 of the Federal Constitution.

Data protection is aimed at protecting the individual from his/her fundamental right to informational self-determination being violated.

YOUR WORKPLACE

While working at KIT, you will usually come into contact with personal data.

Workstations and other modern IT devices as well as many software packages and programs supplied enable you to electronically, i.e. automatically, process personal data.



According to the GDPR, however, not only automatic data processing is subject to data protection regulations. Data protection regulations also apply to data stored in a file system, i.e. in a collection of personal data structured according to certain criteria, such as records in a registry.

As these types of data processing may violate the general right to the protection of personality of data subjects, greatest care should be taken when handling personal data.

PERSONAL DATA

From the point of view of data protection, the question of admissibility of data processing arises whenever personal data are handled.

What Are Personal Data?

Personal data means any information relating to an identified or identifiable natural person.

An identifiable natural person is a person who can be identified, directly or indirectly, in particular by reference to an identifier, such as a name, identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person (Article 4, No. 1 GDPR).

The scope of the term “personal” is accordingly wide. Data are personal already, if they allow a certain person to be identified from a single data item or from several single data items together.

Examples of Personal Data:

- Last name, first name
- Address
- Age
- Date of birth
- Civil status
- Telephone number
- Email address
- Student ID number
- Personnel number
- Holiday times
- Health data
- Data on income or assets
- Data on political or religious denominations or memberships with other social institutions.



LEGAL REGULATIONS

Any processing of personal data of colleagues, students, partners in science, or any other person is subject to data protection regulations.

Processing means any process ranging from the collection of personal data to storage, to modification or other use, to disclosure by transmission, to deletion.

The existing legal provisions are supposed to provide clarity:

- ➔ Clarity for you when processing data; you know what you are allowed to do and which obligations you have.
- ➔ Clarity for you as a data subject; you know what you have accept and which rights you have.

The most important regulations applicable to you are, among others:

- The EU General Data Protection Regulation (GDPR)
- Landesdatenschutzgesetz Baden-Württemberg (State Data Protection Act of the State of Baden-Württemberg)
- Landeshochschulgesetz (LHG, Higher Education Act of the State of Baden-Württemberg) in conjunction with the Hochschul-Datenschutzverordnung (Data Protection Regulation for Higher Education of the State of Baden-Württemberg)
- Telekommunikationsgesetz (TKG, Telecommunication Act).

DATA SECRECY

According to Article 3, par. 2 LDSG, you are obliged to observe data secrecy:

“Den bei öffentlichen Stellen beschäftigten Personen ist es untersagt, personenbezogene Daten unbefugt zu verarbeiten (Datengeheimnis). Das Datengeheimnis besteht auch nach Beendigung ihrer Tätigkeit fort.“ (It is forbidden to persons employed by public institutions to process personal data unauthorized (data secrecy). Data secrecy shall continue to be valid even after the end of their employment.)

DATA PROTECTION PRINCIPLES

The following principles represent basic rules you have to observe whenever you process personal data.

■ Lawfulness of Data Processing

Processing of personal data is lawful when it takes place with the approval of the data subject or on the basis of another permissible legal provision.

Example: Applicants for a university place have to provide various personal data for admission. The legal basis is the Higher Education Act of the State of Baden-Württemberg in conjunction with the Data Protection Regulation for Higher Education of the State of Baden-Württemberg.

■ Fairness

It is referred to the general obligation to be fair and to consider the interests and expectations of the data subject in connection with the processing of personal data.

■ Transparency

The principle of transparency represents a special expression of the principle of fair and lawful processing. The data subject must be able to retrace whether, by whom, and for which purpose his/her personal data are processed.

In this connection, the data subject must receive information on the processing of personal data. This information has to be precise, easily accessible, understandable, and written in a clear and simple language.

Example: For voluntary participation in a scientific study, the institute in charge of this study needs your declaration of consent. The text of this declaration has to clearly and unmistakably outline to which form of processing of your personal data you agree. Further important

information on the processing of your personal data is contained in the corresponding information on data protection (Privacy Policy).

■ Purpose Limitation

Personal data may only be collected for the purposes defined for the execution of tasks and must not be processed further in a way that is not compatible with these purposes.

Example: For assessing the needed childcare places, you have given your contact data to the responsible department in order to be informed about latest news. These data may only be processed for this purpose and not for any other purpose, such as advertising for a planned training course on "Compatibility of Job and Family."

■ Data Minimization (Principle of Necessity)

Personal data may only be processed, if this is absolutely necessary for executing the tasks and in a reasonable relation to the purpose pursued.

Data collection must be limited to the extent absolutely required for the purposes of processing. If data are useful or helpful only, the principle of necessity is not fulfilled.

Example 1: For executing the tasks at the workplace, not all staff members of a department need to know all dates of birth. It is not permitted to make available to all staff members in the department a list with all dates of birth of the colleagues.

Example 2: Within the framework of a scientific study, it is not always required for the concrete purpose of the research project to store the address data of test subjects.

■ Data Accuracy

The personal data processed must be correct and updated to the extent required for processing. If the data are incorrect for the purposes of processing, they have to be deleted or corrected immediately.

Example: If your last name has changed as a result of your marriage, the new name has to be stored in the personnel administration system. Otherwise, your data above would be incorrect.

■ Storage Limitation (Data Economy over Time)

Data allowing for the identification of a person may only be stored as long as this is required for achieving the purpose. Storage duration is to be limited to the absolutely required minimum.

Example: For the retention of invoice documents, certain retention periods are specified in the Commercial Code (HGB). Upon the expiry of these periods, the documents have to be destroyed and stored data must be deleted.

Subject to the execution of appropriate technical and organizational measures, personal data processed for scientific research purposes, for instance, may be stored for a longer period of time.

■ Integrity and Confidentiality

Personal data must be processed such that their security and confidentiality are sufficiently guaranteed. For this, adequate technical and organizational measures have to be taken.

During your daily work, you can contribute to a security-conscious use of personal data by taking a few measures. More details are given in "Practical Tips for Your Workplace."

YOUR RIGHTS AS A DATA SUBJECT

According to the GDPR, you have the following rights vis-à-vis KIT as far as your personal data are concerned:

- Right of information
- Right of access
- Right to rectification and erasure
- Right to restriction of processing
- Right to object to processing (depending on the individual case)
- Right to data portability (depending on the individual case)
- Right to lodge a complaint with the supervisory authority

Please bear in mind:

The rights you have as a data subject also represent obligations as soon as you process personal data at KIT. In particular, the information obligation has to be observed.



Practical Tips for Your Workplace

*What can I do?
What should I never do?*

When using information and communication technology as well as infrastructure for digital information processing, the most important principle is to be security-conscious.

In the sections below you will find selected recommendations and rules of conduct in connection with the processing of personal data at KIT. These are intended to provide first orientation. If you have any further questions, contact the Data Protection Staff Unit (DSB).

Inquiries Relating to Persons

If requested by phone or by uncoded email, do not provide any data, unless you have critically checked legitimacy in advance. Point out in principle that inquiries in writing only (also by fax) will be answered exclusively.

In case of inquiries by investigation authorities, information may only be provided via the Legal Affairs Business Unit (RECHT). In case of inquiries by other authorities, please contact the Data Protection Staff Unit (DSB).

Personal Data of Employees

Personal data of employees may only be processed, if this is required for establishing, executing, and terminating employment relationships or for in-house staff planning or if this is required by a legal provision, a collective agreement, or a service agreement. Personal data of employees may only be accessed by employees, if they are necessary for fulfilling their tasks. At KIT, the Human Resources Business Unit (PSE) is responsible for personnel file data in principle.

Data of Students

Do not publish any student ID numbers, groupings, dates of examinations or lists of grades with student ID numbers on the internet. Publication of data of students, such as the subjects of their graduation theses, on the internet, require the students' approval.

Data Protection at Your Office

Lock your office even in case of short absences. Especially in offices open to the public, keep your documents such that they are not visible to others. Use lockable cabinets and keep them locked when confidential data are stored there.

Waste Disposal Services of KIT

Use KIT's services for the disposal of confidential documents and materials relevant to data protection. The Waste Management Center (phone 608-22222) is responsible for waste management and answers the corresponding questions.

Right to the Personal Image

Publication of photos of employees on the internet, intranet or on paper requires their approval in principle. In cases of doubt, contact the Data Protection Staff Unit (DSB).

Sending Emails to Several Recipients

Use the BCC function of your mail program when sending emails to several recipients. In this way, the recipients will not see the addresses of the other recipients.

Non-encrypted Email is like a Postcard

On their way from the sender to the addressee, emails may be read or even modified by any number of persons. Personal data or other information worth protecting must not be sent by non-encrypted email. At KIT, it is possible to send, receive, and sign encoded encrypted emails.

Please bear in mind that when sending an encrypted email the text in the subject line continues to be displayed.

Information on sending confidential data by email and on applying for the certificates necessary for this purpose may be obtained at http://intranet.kit.edu/downloads/2014_CIO_DSB_E-Mailversand_vertraulicher_Daten.pdf (in German). You can apply online for your user certificate with SCC at <https://www.ca.kit.edu/english/index.php>.

Password Protection

Your computer is provided with a password protection. You specify your password (see password regulation of SCC at <http://www.scc.kit.edu/en/services/4319.php>). The password is the key to your computer and data. Whoever has this key, may use or misuse your data in your name!

Therefore, keep your authentication information secret, also to your superiors and colleagues. In an emergency, an administrator can provide an authorized person with access to his/her data in a regulated procedure.

Automatic Screen Lock

Lock your screen whenever you leave your workplace. When using Windows, this can be done quickly by pressing the Windows key+L together. Also set the automatic screen lock of your PC.

Protection against Malware

Risks due to malware, such as viruses, worms, or Trojans, cannot be excluded in principle. Computers therefore have to be provided with an appropriate antivirus program.

SCC supplies a central antivirus service (<http://www.scc.kit.edu/dienste/virenschutz.php>) (in German).

Loss and Destruction of Data

To prevent loss of data – unintended or caused without authorization –, data can be secured on external data carriers. Secure storage and controlled disposal of paper printouts and other storage media must be ensured.

SCC supplies a central data backup service (<http://www.scc.kit.edu/en/services/6161.php>).

If you have questions relating to IT, contact the IT Commissioners at the institutes or the Steinbuch Centre for Computing (SCC).

Useful information on IT security at KIT can also be found on the intranet of KIT at <https://www.itsb.kit.edu> (in German) or <https://www.cert.kit.edu/english/index.php>.



Obligation to Report Personal Data Breach

According to the GDPR, KIT is obliged to notify a personal data breach to the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of it (Art. 33 GDPR), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons. Moreover, KIT is obliged to communicate the personal data breach to the data subject when the personal data breach is likely to result in a high risk to this person's rights and freedoms (Art. 34 GDPR).

In case an incident occurs in connection with your work at KIT, which may result in a personal data breach, immediately inform the Head of your Organizational Unit.

Training Courses on the Fundamentals of Data Protection

Employees working at KIT for a period longer than four months have to pass a training course on the fundamentals of data protection every three years.

KIT offers this training in the form of an e-learning course. You will be invited automatically by email and do not have to make any arrangements for yourself.

Whenever you have questions relating to the processing of personal data:

Contact your Data Protection Commissioner and/or the team of the Data Protection Staff Unit (DSB).

Useful information on data protection can also be found on KIT's intranet at <http://www.dsb.kit.edu> (in German).

Contact

Karlsruhe Institute of Technology (KIT)

Datenschutzbeauftragte

Ass. jur. Marina Bitmann

Phone: +49 721 608-41057

Email: marina.bitmann@kit.edu

www.dsb.kit.edu

Issued by

Karlsruhe Institute of Technology (KIT)

President Prof. Dr. Jan S. Hesthaven

Kaiserstraße 12

76131 Karlsruhe, Germany

www.kit.edu

Karlsruhe © KIT 2026